Secretariat

16 August 2021

Administrative instruction

Issuance, retention and disposal of communications and information technology assets

1. Pursuant to rule 7.1 of the Financial Rules of the International Seabed Authority the Secretary-General promulgates the following:

Section 1
Purposes and objectives

2. The purpose of the present instruction is to establish procedures relating to the issuance, retention and disposal of communications and information technology (CIT) assets that are the property of the International Seabed Authority and to set out the respective responsibilities of the Communications and Information Technology Unit and staff members in that regard, including the loss of or damage to CIT assets.

3. The objectives of the present instruction are not only to enable the CIT Unit to track the locations of CIT assets and who is using them, but also to ensure the security of the Authority's network, protect any data stored on those assets from any risk of breach or loss and ensure that CIT assets are disposed in conformity with the applicable financial rules.

Section 2
Issuance of communications and information technology assets

4. All CIT assets should be tagged and added to the Authority's inventory control record, which holds information on and tracks movement of all Authority's properties.

5. For the purpose of the present instruction, the categories and estimated useful lifetime of CIT assets are listed in the annex. Assets that cost less than 75 United States dollars and do not contain data are not required to be specifically tracked. However, all CIT assets that store sensitive data should be tracked, regardless of cost.

6. The CIT assets that are required to be tracked must be assigned an internal tracking number and/or a barcode by the CIT Unit when they are received. Details of those CIT assets, including the name, type, internal tracking number and/or barcode, current user and location and, where appropriate, locations of sensitive data, should be put into the Authority's inventory control record whenever such an asset is delivered, assigned, reassigned, recycled, sold or donated.

7. Staff members should be trained on the use of CIT assets and of confidential information and other policies and procedures relating to the security of data before being issued CIT assets as approved by the heads of offices.

Section 3
Retention and use of communications and information technology assets

8. Staff members must use the CIT assets assigned to them for official purposes only and must exercise reasonable care pursuant to rule 1.6 of the Staff Rules.

9. Staff members who are allocated CIT assets are responsible for their use, maintenance, security and safekeeping. Staff members must at all times comply with the Authority's policy on acceptable use of communications and information resources and data[1] and follow the security guidelines issued by the CIT Unit. In case of misuse of an assigned CIT asset by a staff member, the asset may be withdrawn by the relevant head of office, in consultation with the Director of the Office for Administrative Services.

10. Staff members shall never place sensitive data on a device or any type of media without authorization from the relevant head of office. Once authorization has been obtained, the data-bearing item must be kept in a secure area.

11. Staff members must never use CIT assets to download or install any software without prior authorization from the CIT Unit.

12. Prior to separation from service, staff members shall return all CIT assets in good condition, reasonable wear and tear excepted. The CIT Unit is responsible for maintaining and updating the Authority's inventory control record accordingly.

13. In the case of loss of or damage to any CIT asset, the staff member concerned shall immediately submit a written report to the Director of the Office for Administrative Services, and the CIT Unit will immediately take all measures necessary to minimize the potential loss of sensitive data.

14. Physical verification shall be conducted by the CIT Unit on a regular basis and as deemed necessary to ensure adequate control over CIT assets. The findings of the verification process shall be reconciled with the Authority's inventory control record.

15. In the case of any loss of or damage to CIT assets as a result of negligence on the part of a staff member, the staff member may be required to compensate the Authority accordingly.

Section 4
Disposal of data

16. Prior to disposal of any CIT asset, the CIT Unit must ensure that all organization information and data contained in the asset have been properly removed. The CIT Unit must be informed of the impending disposal of each CIT asset in a timely manner to allow time for the appropriate data and software cleaning exercise. This responsibility must never be delegated to any person outside the Authority. The CIT staff responsible for decommissioning must sign documentation including the brand, make and model of the asset being decommissioned and attesting that all organization information and data were properly removed in accordance with all provisions of the present instruction.

[1] ISBA/ST/SGB/2017/3.

17. Data erasure requirements for each CIT asset are based upon the sensitivity of the data stored on the device as determined during the data assessment process. The CIT Unit shall be responsible for ensuring the clearance of information as follows:

(a) Unclassified data: In the interest of prudence, normally erase the data using any available means, such as software-based data sanitization and physical destruction;

(b) Confidential data: Erase the data using any available means, such as data sanitization or physical destruction. Data may only be removed from secure areas with the permission of the Director of the Office for Administrative Services or the Secretary-General;

(c) Strictly confidential data: The data must be erased using an approved technology or, where necessary, the CIT asset containing such data must be physically destroyed, in order to ensure that data are not recoverable using advanced forensic techniques. Data may only be removed from secure areas with the permission of the Secretary-General.

Section 5
Disposal of communications and information technology assets

18. When a CIT asset has reached the end of its life cycle, or ceases to function, the CIT Unit should evaluate its usefulness and make recommendations to the Director of the Office for Administrative Services regarding the disposal of the CIT asset or its parts.

19. The method of disposal of CIT assets is to be determined by the Secretary-General. Where required by the Financial Rules, the Secretary-General must seek the written advice of the Property Survey Board.

20. Before any CIT assets, in particular computer equipment, laptops and mobile phones, are disposed of, their residual value should be first determined by the Director of the Office for Administrative Services, on the basis of a valuation by the Budget and Finance Unit, taking into account the age of the asset, its lifetime expectancy and depreciation.

21. When disposing of CIT assets, the following options should be considered:

(a) Recycling: The CIT assets should be decommissioned and recycled in line with environmentally friendly or green initiatives;

(b) Reassignment: Where a CIT asset reaches the end of its life cycle and is inadequate for the designated purpose, but is still in working order, the asset should be reassigned internally, if practical;

(c) Sale: CIT assets with residual value but that are superfluous to the Authority's requirements may be written off and sold. At the discretion of the Secretary-General, the staff member to whom the asset was assigned may be given the option to purchase the asset;

(d) Donation: Where a CIT asset has little or no residual value, consideration may be given to donate it to charity.

Section 6
Final provisions

22. The present instruction shall take effect on the date of its issuance.

(*Signed*) Michael W. **Lodge**
Secretary-General

Annex

Categories of communications and information technology assets and their useful life

Asset classes	*Asset subclass*	*Equipment type*	*Estimated useful lifetime (in years)*
Communications and information technology equipment	**Information technology equipment**	Desktop workstations	4
		Laptops, tablets and iPads	4
		Printers, copiers, scanners, fax machines and multifunction machines	4
		Memory devices and external hard drives	3
		Servers	4
		Firewalls	3
		Routers and switches	4
		Switches	4
	Communications equipment	Mobile phones	3
		Handheld devices	4
	Audiovisual equipment	Sound systems and cameras	5